UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,657	11/26/2003	Jayme Matthew Fishman	13230-103	8773

26486 7590 01/31/2007

BURNS & LEVINSON, LLP
(FORMERLY PERKINS SMITH & COHEN LLP)
125 SUMMER STREET
BOSTON, MA 02110

EXAMINER	
HOANG, DANIEL L	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/723,657	FISHMAN ET AL.	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/26/03, 3/23/06*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/23/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-19, 23-24, 27-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Marchant, US Patent No. 6,240,183.

As per claim 1, 5-12, 23, 24, Marchant teaches:

A system for authentication of a party comprising:

> *[see col. 2, lines 1-3] "a security unit and technique is disclosed that attaches outside of a user's computer and assists in decrypting encrypted information using random encryption algorithms."*
>
> *Examiner interprets the user as the party being authenticated and further that authentication is attained by successful decryption of encrypted information.*

an authentication server associating a unique set of information with said party,

> *[see col. 2, lines 5-10] "The security unit attaches conveniently to an easily accessible port of a laptop or desktop computer and includes an encryption schema which is a random array of bits. The same encryption schema is also stored at the data site where the secure data originates before it is transmitted to the user's computer."*
>
> *The data site is associated with a server which examiner is interpreting as the "authentication server" in applicant's claim. In regards to the claimed "unique set of information", examiner is interpreting that to be the encryption schema. As is evident above, both server and party have access to the same unique set of information.*

said unique set including at least a unique ordered set of information randomly generated;

> *[see col. 6, line 51] "Encryption schema 204 is a random array of bits."*

responsive to receipt of identifying information *[password or PIN]* of said party

> *[see col. 7, lines 6-11] "The user begins by establishing communication between his computer 102 and the data site 62. When the user desires to access secure information, he transmits a password to the data site to permit the data site to identify the unique encryption schema that is also present within the user security unit 52."*

to determine by random generation values of one or more prescribed parameters

[see col. 7, lines 11-13] "The data site then generates and transmits a random public code 206 in the clear to computer 102 so that the user may enter the public code into the security unit."

to define an ordered subset of said ordered set *["encryption schema"]*,

[see col. 11, lines 10-15] "This public code may be any sequence of numbers, letters, and/or symbols that is used to access the encryption schema. Both the data site and the security unit at the user's computer will combine the same user PIN and public code in order to access the same encryption schema. In step 518 the data site combines this public code with the user PIN to obtain an entry point into the encryption schema. This entry point represents a random address into the encryption schema and serves as a starting point for determining the first length of string, encryption algorithm identifier and relative address.

to transmit said values *["random public code"]*,

[see col. 11, lines 11-13] "The data site then generates and transmits a random public code 206 in the clear to computer 102 so that the user may enter the public code into the security unit."

to generate a first token *["encryption algorithm"]* from said ordered subset,

[see col. 11, lines 22-35] "Thus, in step 520 the data site uses this entry point to obtain three sets and subsets of bits that correspond to the first length or lengths of the string to be transmitted, an encryption algorithm identifier or identifiers and a relative address or addresses. One method of obtaining the three sets of bits is where the combined public code and user PIN are then processed through an exclusive OR (XOR) with the first three sets of bits which begin at the entry point. This encrypts the three sets and subsets. The result is then utilized to identify the corresponding lengths, algorithms and relative addresses. In step 522 the data site encrypts a first part of the information to be sent to the user using the encryption algorithm identified by the encryption algorithm identifier bit set."

to compare said first token to a second token received in response to said transmission,

[see col. 12, lines 22-24] "Next, in step 536 the security unit combines the PIN and the public code to obtain an entry point into the encryption schema."

and upon a match, to authenticate said party;

[see col. 12, lines 26-33] "Because the data site has previously combined the same public code and the same PIN using the same combination technique, the entry point obtained by the security unit into the encryption schema will be the same entry point obtained by the data site previously in step 518. Thus, both the data site and the security unit are synchronized with respect to where to begin within the encryption schema for encryption/decryption.

and a separate processor operated by said party adapted to read locally a storage medium containing a copy of said unique set of information associated by said server with said party,

[see above wherein the user's computer is adapted to read information from the security unit which contains an encryption schema.]

to transmit to said server said identifying information,

[see above wherein the user transmits a password or PIN to the server]

to receive said values from said server,

[see above wherein the user receives a public code from the server]

to apply said values to define an ordered subset of said copy, and

[see above wherein the public code is used to derive an encryption/decryption algorithm.]

to transmit said second token generated from said ordered subset of said copy.

[see above wherein the decryption of data is done using the decryption algorithm attained from the security unit.]

As per claim 2, 14, Marchant teaches:

The system of claim 1 wherein said first token includes personal code known to said party and stored and associated with said party at said server and said second token identically includes said personal code entered by said party at said separate processor.

[see rejection of claim 1 above, wherein the encryption/decryption algorithms are derived from the user's PIN which are known and stored with the client as well as the server]

As per claim 3, Marchant teaches:

The system of claim 1 wherein said server further comprises means for, upon said match, generating and storing a transaction token and transmitting to said processor said transaction token;

[see rejection of claim 1, wherein upon sending the server the user's PIN, the server responds with a corresponding public code]

said system further comprising an authentication-seeking entity adapted

[see rejection of claim 1, wherein the claimed "authentication-seeking entity" is the user's computer.]

to receive from said processor said transaction token,

[see rejection of claim 1, wherein the user is adapted to receive the public code used to attain the proper encryption/decryption algorithm.]

to transmit said transaction token to said server, and

[see rejection of claim 1, wherein the PIN is combined with the public code to attain the proper encryption/decryption algorithm so user may communicate with server securely.]

to receive from said server authentication upon match by said server of said stored transaction token with said transmitted transaction token.

[see rejection of claim 1, wherein authentication is attained through successful decryption of encrypted information.]

As per claim 4, Marchant teaches:

The system of claim 1 further comprising an authentication-seeking entity adapted to receive from said processor said second token, to transmit said second token to said server, and to receive from said server authentication upon match by said server of said first token.

[see rejection of claim 1, wherein the user's computer utilizes the security unit in order to derive an encryption/decryption algorithm in which it uses to decrypt encrypted information transmitted from the server.]

As per claim 13, Marchant teaches:

A process for authenticating a party comprising

selection at a central location of a randomly selected portion of random information uniquely associated with said party,

[see rejection of claim 1 wherein the claimed "central location" is the server, "randomly selected portion" is the encryption/decryption algorithm, and "random information uniquely associated with said party" is the encryption schema.]

parallel selection at a party location separate from said central location an identical portion of a putatively identical copy of said information issued to and possessed by said party, and

[see rejection of claim 1, wherein the claimed "party location" is the security unit located at the user's computer, "identical portion" is the encryption/decryption algorithm residing in the security unit, and "information issued to and possessed by said party" is encryption schema.]

comparison at said central location of a first token uniquely generated from said randomly selected portion with a second token uniquely generated from said identically selected portion.

[see rejection of claim 1, wherein an encryption algorithm is derived at the server and used to encrypt information sent to the user, further wherein the user utilizes the security unit to derive a decryption algorithm that can be used to decrypt said encrypted information.]

As per claim 15, Marchant teaches:

A process for authenticating a party comprising the steps of:

(a) accessing by said party through a client computer of an authentication server that has stored random information uniquely associated with said party, a copy of which was previously provided to said party and accessible at the client side;

[see rejection of claim 1, wherein claimed "party" is the user, "client computer" is the user's computer, "authentication server" is the server comprising a data site, "random information uniquely associated with said party" is the encryption schema which is associated with the user through use of a user PIN and pubic code, and further a copy of encryption schema resides at said user within the security unit that is attached to user's computer.]

(b) generating by said server or said client at least one random value for an authentication session of a parameter for selecting an ordered subset of said stored random information;

[see rejection of claim 1, wherein the claimed "random value" is the randomly generated public code which is combined with the user PIN to derive an encryption algorithm from the encryption schema. The claimed "ordered subset" is the encryption algorithm

(c) transmitting by said server or client respectively to said client or server said generated value;

[see rejection of claim 1, wherein the public code is transmitted to the user.]

(d) applying by said client said generated value or values to select an ordered subset of said copy information;

[see rejection of claim 1, wherein the user also uses its PIN combined with the public code to select a decryption algorithm from the encryption schema contained in the security unit.]

(e) generating by said client from said ordered subset of copy information a client-side party-authenticating token;

[see rejection of claim 1 wherein the decryption algorithm is generated.]

(f) applying by said server of said generated value or values to select an ordered subset of said stored information;

[see rejection of claim 1, wherein the server uses the user's PIN combined with a randomly generated public code to select an encryption algorithm from the encryption schema.]

(g) generating by said server from said ordered subset of stored information a server-side party-authenticating token;

[see rejection of claim 1, wherein the encryption algorithm is generated by the server.]

(h) transmitting by said client to said server said client-side token or by said server to said client said server-side token; and

[see rejection of claim 1, wherein the encryption algorithm is used to encrypt information which is sent to the user.]

(i) comparing by said server said client-side token with said server-side token or by said client said server-side token with said client-side token.

[see rejection of claim 1, wherein the encrypted information is decrypted using a decryption algorithm generated by the user.]

As per claim 16, 18, 19, Marchant teaches:

The process of claim 15 wherein step (b) comprises the steps of generating random values for an offset, a length and a shift; and

[see col. 9, lines 55-67] "Once an encryption schema has been identified for a particular security unit, the data site in step 456 then agrees upon a convention to use for the sets of bits that will be accessed within the encryption schema. The data site identifies the number of bits to be used to represent the "length of string", the "encryption algorithm identifier", and the "relative address". The data site also identifies the relative location of these three sets of bits in relation to an entry point indicated by the address register. As an illustrative example, FIG. 6 shows that in one embodiment each of the three sets of bits is 8 bits in length and they begin at the location indicated by the address register and follow consecutively thereon. Of course, other conventions are possible."

steps (e) and (g) each comprise the step of applying a specified one-way hashing algorithm to generate respectively said client-side and server-side party-authenticating tokens.

[see col. 20, lines 38-45] "the encryption/decryption algorithms can include any method of encryption/decryption such as: salting, and bit/byte manipulation, bit/byte substitution, exchanging bits/bytes, ORing bits, exclusive Oring, ANDing bits, character transformation, character movement or combinations of these or any other more complex encryption schemes for encrypting information not requiring transmission of a key together with the encrypted information.

As per claim 17, Marchant teaches:

The process of claim 15 wherein a copy of personal code known to said party is stored and associated with said party at said server and wherein step (e) further comprises the steps of

(l) concatenating said ordered subset of copy information and said personal code entered by said party and

[see rejection of claim 1, wherein the user PIN is combined with the public code to derive the encryption algorithm at the server.]

(ll) applying a specified one-way hashing algorithm to generate said client-side party-authenticating token; and step (g) further comprises the steps of

[see rejection of claim 16 above]

(l) concatenating said ordered subset of stored random information and said personal code copy and

[see rejection of claim 1, wherein the security unit residing at the user's computer combine's the user's PIN with the public code to derive the decryption algorithm.]

(ll) applying said specified one-way hashing algorithm to generate said server-side party-authenticating token.

[see rejection of claim 16 above]

As per claims 27-28, Marchant teaches:

The process of claim 15 applied to authenticating said party for access to a restricted resource wherein, if step (i) results in a match, said process further comprises the step of (j) transmitting by said server authorization to permit said access.

The Marchant reference has been discussed above. The claimed "restricted resource" is interpreted by examiner to be equivalent to Marchant's encrypted information.

As per claims 27-28, Marchant teaches:

The process of claim 15 applied to authenticating said party for continuing access to a restricted resource wherein said copy is normally separate from and inaccessible by said client except when connected through action of said party and steps (b) through (i) are repeated periodically until step (i) fails to result in a match a predetermined number of times.

[see rejection of claim 1, wherein the security unit is kept outside of user's computer and information contained in the security unit is only accessible through the correct combination of both the user's PIN and the server's public code.]

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marchant as applied to claim 15 above, and further in view of Ganesan, US Patent No. 5,557,678.

As per claim 20:

The process of claim 15 wherein a copy of personal code known to said party is stored and associated with said party at said server and wherein step

(e) further comprises the steps of

> (I) dividing said ordered subset of copy information into first and second portions;
>
> (II) concatenating each of said first and second portions with said personal code entered by said party;
>
> (III) applying a specified one-way hashing algorithm to said concatenation of said first portion to generate said client-side party-authenticating token; and
>
> (IV) applying said specified one-way hashing algorithm to said concatenation of said second portion to generate a second client-side party-authenticating token;

step (g) further comprises the steps of

> (I) dividing said ordered subset of stored random information into first and second portions corresponding to said first and second portions of step (b);

(II) concatenating each of said first and second portions of this step with said personal code copy;

(III) applying said specified one-way hashing algorithm to said concatenation of said first portion to generate said server-side party-authenticating token; and

(IV) applying said specified one-way hashing algorithm to said concatenation of said second portion to generate a second server-side party-authenticating token;

step (h) is performed by said client;

step (i) is performed by said server; and, wherein, if step (i) results in a match, said process further comprises the steps of

(j) transmitting by said server to said client said second server-side token; and

(k) comparing by said client of said server-side token with said client-side token.

The Marchant reference has been discussed above and reads upon all limitations of claim 20 except for the following:

(I) dividing said ordered subset of copy information into first and second portions;

(I) dividing said ordered subset of stored random information into first and second portions corresponding to said first and second portions of step (b);

As has been discussed above, Marchant teaches of an ordered subset of copy information as well as an ordered set of stored random information. Marchant does not explicitly disclose dividing said information into first and second portions. The Ganesan reference teaches the following:

> *[see col. 3, lines 55-60] "a first and second user private encryption key and a corresponding first and second user public encryption key for a respective first and second user of a split key public cryptosystem are generated. The private encryption keys are divided into first and second user key portions and corresponding first and second central authority key portions. The first and second user key portions are respectively disclosed to the first and second users. The central authority key portions and public encryption keys are disclosed to a central authority."*

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Marchant reference to incorporate the above teachings of Ganesan to divide the information into two portions. Doing so would improve upon the overall security of the system because an attacker would have to obtain both portions of the information in order to perform successful decryption.

As per claim 21:

The process of claim 20 wherein step (b) comprises the steps of generating random values for an offset, a length and a shift.

[see rejection of claim 16]

As per claim 22:

The process of claim 21 wherein step (b) further comprises selection of a one-way hash algorithm.

[see rejection of claim 16]

Claims 25-26 rejected under 35 U.S.C. 103(a) as being unpatentable over Marchant.

As per claim 25, Marchant teaches:

The process of claim 15 applied to authenticating work product that said party creates or modifies using said client computer wherein,

if step (i) results in a match, said process further comprises the steps of

[see rejection of claim 1, correct user PIN/password]

(j) generating by said server a work-product-authentication token;

[see rejection of claim 1, generation of public code]

(k) storing at said server a copy of said work-product-authentication token associated with said party;

[see rejection of claim 1, server stores a copy of public code]

(l) attaching to said work product said work-product-authentication token to create a data object stored and movable as authenticated work product;

[see rejection of claim 1, encrypted information sent to user with public code]

(m) storing said authenticated work product;

*[see rejection of claim 1, the encrypted information is stored at the client computer to be decrypted
]*

(n) extracting from said authenticated work product a putative work-product authentication token; and

[see rejection of claim 1, wherein user combines the public code with the user PIN to access the security unit to derive a decryption algorithm used to decrypted the encrypted information.]

(o) comparing at said server said stored work-product-authentication token with said putative work-product-authentication token.

[see rejection of claim 1, wherein decrypted information on user's computer should match original unencrypted information on server if the correct decryption algorithm was derived and applied.]

The Marchant reference has been discussed above. Marchant teaches the claimed embodiments above, except Marchant does not explicitly teach that the system is applied to authenticating work products. It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to apply the teachings of Marchant in order to authenticate work products. One would be motivated to do this in order to protect said work products from unauthorized access.

As per claim 26, Marchant teaches:

The process of claim 15 applied to authenticating work product that said party creates or modifies using said client computer wherein,

[see rejection of claim 25 and application towards work products]

[see col. 4, lines 38-39] "Computer system 12 that receives and/or transmits encrypted messages."

if step (i) results in a match, said process further comprises the steps of

[user submission of PIN]

(j) generating by said server a server-side work-product-authentication token from information associated with said party and stored at said server;

[server generates a encryption/decryption algorithm]

(k) transmitting by said server to said client information to specify parallel generation by said client of a client-side work-product-authentication token from corresponding information made available at said client;

[server sends user a public code that can be used to generate a matching encryption/decryption algorithm from encryption schema available on user's security unit.]

(l) generating by said client said client-side work-product-authentication token from said corresponding information;

[user utilizes PIN and received public code to derive an encryption/decryption algorithm.]

(m) attaching to said work product said client-side work-product-authentication token to create a data object stored and movable as authenticated work product;

[user encrypts information to be sent to server using encryption algorithm derived in previous step]

(n) storing said authenticated work product;

[encrypted information is stored and transmitted to server.]

(o) extracting from said authenticated work product said client-side work-product authentication token; and

[using server public code and matching user's PIN, the server can access its own copy of user's encryption schema to attain a proper decryption algorithm and decrypt encrypted information]

(p) comparing at said server said serve-side work-product-authentication token with said client-side work-product-authentication token.

[server decryption algorithm should match user's encryption algorithm if correct PIN and public code are used and proper decryption algorithm is attained from encryption schema.]

Conclusion

The following patents are cited to further show the state of the art with respect to transaction authentication

US Patent No. 6684330 to Wack, which is cited to show cryptographic information and flow control.

US Patent No. 6542608 to Scheidt, which is cited to show a cryptographic key split combiner.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang
1/26/07

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/29/07